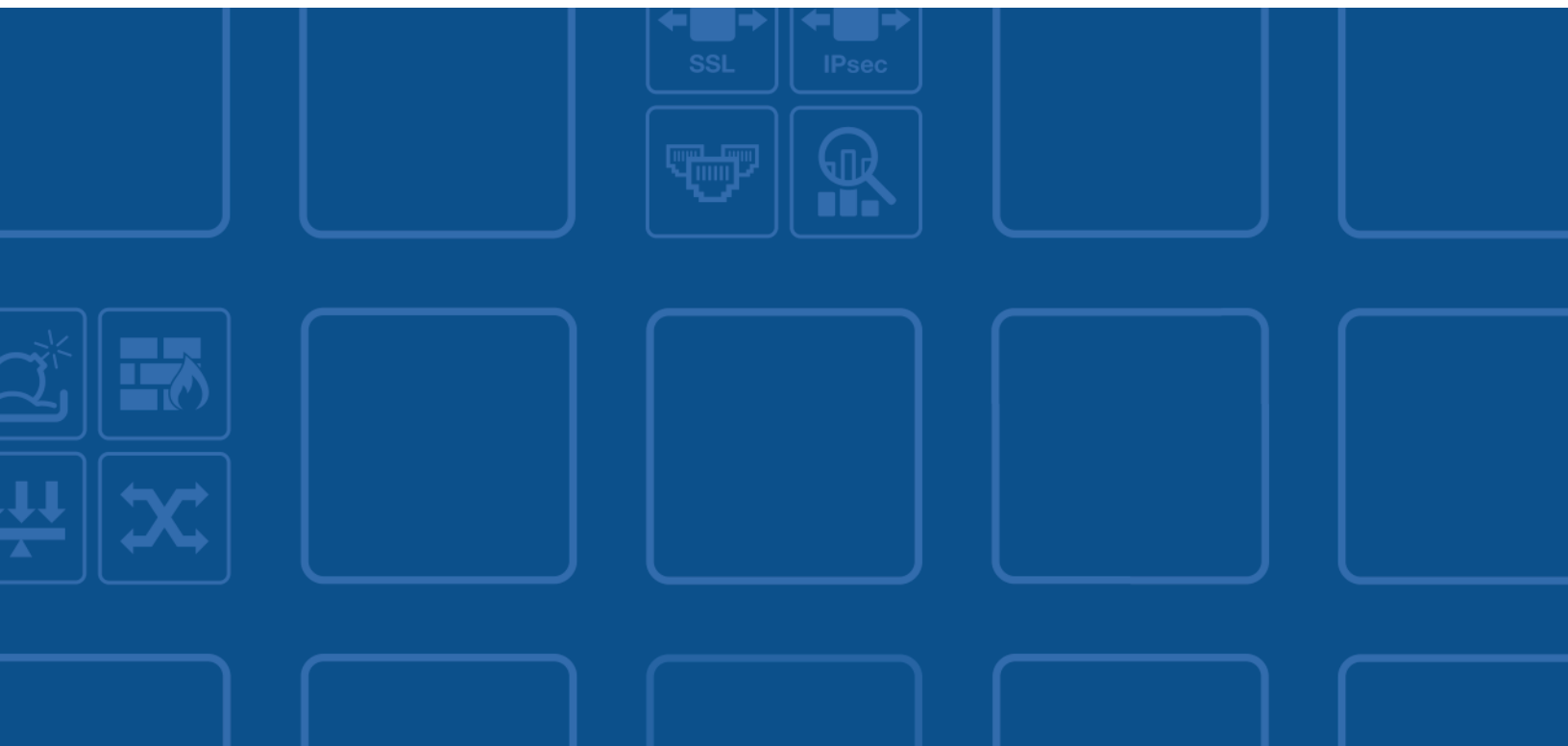
FORTINET
High Performance Network Security

FortiManager - Release Notes

VERSION 5.4.1



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 29, 2016

FortiManager - Release Notes

02-541-370565-20161229

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-06-29	Updated for 5.4.1 release
2016-07-05	Updated to add support for FortiOS 5.2.8 and 378564 as a known issue
2016-07-07	Updated to add a special notice and the following known issues: 379088, 375575.
2016-08-03	Updated to add the following known issues: 379245, 380336, 375204.
2016-09-01	Updated to remove support for 32-bit VMs.
2016-09-20	Updated to add the following known issue: 388071.
2016-09-30	Updated to add the following resolved issue: 371045.
2016-10-11	Updated to add support for FortiOS 5.2.9.
2016-11-15	Updated to add cross-reference between FortiDDoS in the FortiManager Support table and the Feature Support table.
2016-11-25	Updated to add support for FortiOS 5.4.2.
2016-11-30	Updated to add support for FortiOS 5.2.10.
2016-12-08	Updated description of 397220.
2016-12-15	Updated FortiGuard Center Update Support section to include FortiClient 5.4.0 and later.
2016-12-21	Updated to add support for FortiOS 5.4.3.
2016-12-29	Added special notice about Hyper-V FortiManager-VM running on an AMD CPU.

Introduction

This document provides the following information for FortiManager 5.4.1 build 1082:

For more information on upgrading your device, see the FortiManager *Upgrade Guide*.

Supported models

FortiManager version 5.4.1 supports the following models:

FortiManager	FMG-200D, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000C, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E.
FortiManager VM	FMG-VM64, FMG-VM64-Azure, FMG-VM64-XEN (for both Citrix and Open Source Xen), FMG-VM64-KVM, FMG-VM64-AWS, and FMG-VM64-HV.

What's new in FortiManager 5.4.1

The following is a list of new features and enhancements in 5.4.1. For details, see the *FortiManager Administrator Guide*:

Not all features/enhancements listed below are supported on all models

FortiAP Management

Central Profiles and Monitoring

Improved organization of large AP environments, which includes a simplified workflow and layout of settings and monitored statistics. The full AP health dashboard is now available inside the FortiManager AP Manager component.

Google Map Support

Google map support for location management of APs

AP Groups

Ability to organize all APs into groups for applying common configuration profiles or monitoring templates

Provisioning

Automatically Promote Model Device

Support for zero-touch on-site FortiGate deployment by automatically promoting a model device to a managed device. First you add the model device to FortiManager by using the serial number. Later when the device with that serial number connects to FortiManager, the device is automatically promoted and a configuration applied.

VPN Manager

New Wizard

A new VPN wizard is available to help you easily provision and configure VPNs. The new wizard includes all of the previous wizard functions, plus certificate-based deployments, in a more user friendly (graphical) format.

Migration

Backup and Restore Between Models

Ability to restore the database backup file from one platform to a different platform

Upgrade

One-Step ADOM Upgrade to 5.4

One-step migration procedure to convert a 5.2-based ADOM to a 5.4-based ADOM

Secure DNS Server

Support for running FortiGuard Secure DNS service on FortiManager. Enabling FortiManager Secure DNS service requires installing a dedicated software build and a license.

VM Support

Microsoft Azure Cloud

FortiManager/FortiAnalyzer VM is now available from Azure Cloud.

Support for 32-bit VMs Removed

FortiManager/FortiAnalyzer no longer support 32-bit VMs. For FortiManager, you can use the migration feature to back up and restore between 32-bit and 64-bit VMs. For information, see the *Migrating the Configuration* section in the *FortiManager Administration Guide*.

New GUI Themes Support

Multiple color themes are now available for the FortiManager GUI.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 5.4.1.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

System Configuration or VM License is Lost after Upgrade

When upgrading FortiManager from 5.4.0 to 5.4.1, it is imperative to reboot the unit before installing the 5.4.1 firmware image. Please see the *FortiManager Upgrade Guide* for details about upgrading. Otherwise, FortiManager may lose system configuration or VM license after upgrade. There are two options to recover the FortiManager unit:

1. Reconfigure the system configuration or add VM license via CLI with `execute add-vm-license <vm license>`.
2. Restore the 5.4.0 backup and upgrade to 5.4.1.

FortiOS 5.4.0 Support

With the enhancement in password encryption, FortiManager 5.4.1 no longer supports FortiOS 5.4.0. Please upgrade FortiGate to 5.4.1.

The following ADOM versions are not affected: 5.0 and 5.2.

Local in-policy after upgrade

After upgrading to FortiManager 5.4.1, you must import or reconfigure local in-policy entries. Otherwise, the subsequent install of policy packages to FortiGate will purge the local in-policy entries on FortiGate.

ADOM for FortiGate 4.3 Devices

FortiManager 5.4 no longer supports FortiGate 4.3 devices. FortiManager cannot manage the devices after the upgrade. To continue managing those devices, please upgrade all FortiGate 4.3 to a supported version, retrieve

the latest configuration from the devices, and move the devices to an ADOM database with the corresponding version.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
   set ssl-protocol t1sv1
end
```

Upgrade Information

Upgrading to FortiManager 5.4.1

You can upgrade FortiManager 5.2.0 or later directly to 5.4.1. If you are upgrading from versions earlier than 5.2.0, you will need to upgrade to FortiManager 5.2 first. (We recommend that you upgrade to 5.2.7, the latest version of FortiManager 5.2.)

For details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

During upgrade from 5.2.4 or earlier, invalid dynamic mappings and duplicate package settings are removed from the ADOM database. Please allow sufficient time for the upgrade to complete.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager product data sheet available on the Fortinet web site, http://www.-fortinet.com/products/fortimanager/virtualappliances.html. VM installation guides are available in the Fortinet Document Library.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

FortiManager 5.4.1 support

The following table lists 5.4.1 product integration and support information:

Web Browsers	• Microsoft Internet Explorer 11.0 • Mozilla Firefox version 46 • Google Chrome version 50 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS/FortiOS Carrier	• 5.4.3 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.3, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.3 on page 25. • 5.4.1 to 5.4. FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.4.2, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.4.2 on page 25. • 5.2.8 to 5.2.10 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.8/5.2.9/5.2.10, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.8/5.2.9 on page 26 and Compatibility issues with FortiOS 5.2.10 on page 25. • 5.2.7 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.7, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.7 on page 26. • 5.2.6 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.6, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.6 on page 26. • 5.2.2 to 5.2.5 • 5.2.1 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.1, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.2.1 on page 26. • 5.2.0 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.2.0, with some minor interoperability issues .For information, see Compatibility issues with FortiOS 5.2.0 on page 27. • 5.0.4 to 5.0.12 FortiManager 5.4.1 is fully tested as compatible with FortiOS/FortiOS Carrier 5.0.4 to 5.0.12, with some minor interoperability issues. For information, see Compatibility issues with FortiOS 5.0.4 on page 27.

FortiAnalyzer	• 5.4.0 to 5.4.1 • 5.2.0 to 5.2.5 • 5.0.0 to 5.0.11
FortiCache	• 4.0.0 to 4.0.3
FortiClient	• 5.4.0 • 5.2.0 and later
FortiMail	• 5.3.3 • 5.2.8 • 5.1.6 • 5.0.10
FortiSandbox	• 2.2.1 • 2.1.2 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.2.3 • 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.5.3 • 5.4.1 • 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6
FortiDDoS	• 4.2.1 • 4.1.11 Limited support. For more information, see Feature support on page 16.

Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS
	• Citrix XenServer 6.2
	• Linux KVM Redhat 6.5
	• Microsoft Azure
	• Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2
	• OpenSource XenServer 4.2.5
	• VMware
	  • ESX versions 4.0 and 4.1
	  • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0

To confirm that a device model or firmware version is supported by current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer				
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox	✓	✓		✓
FortiSwitch ATCA	✓			

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiWeb		✓	✓	✓
Syslog				✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiManager CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, and FortiCache models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 5.4.1.

FortiGate models

Model	Firmware Version
FortiGate: FG-80C-DC, FG-80C-LENC, FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-3G4G-NAEU, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80C-LENC, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-101E, FG-140D, FG-140D-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FGT-280D-POE, FGT-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-2000E, FG-2500E, FG 3800D **FortiGate 5000 Series:** FG-5001C, FG-5001D **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-1000C-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810D-DC **FortiGate Low Encryption:** FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-51E, FWF-30D-POE, FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE, FWF-92D, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600D, FG-900D, FG-600C, FG-620B, FG-621B, FG-800C, FG-800D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C,FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:** FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM-Azure, FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-700D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B **FortiGate 5000 Series:** FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C **FortiGate DC:** FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC **FortiGate Low Encryption:** FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC **FortiWiFi:**FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.0

FortiCarrier Models

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3810D-DC, FCR-3815D-DC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND	5.2
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C **FortiCarrier DC:** FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64	5.0

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-2000E, FE-3000E, FE-3200E, FE-VM64, FE-VM64-HV, FE-VM64-XEN **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.3
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1.6
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0.10

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.0
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.3
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.8
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64	4.0

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in 5.4.1.

Compatibility issues with FortiOS 5.4.3

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS 5.4.3.

Bug ID	Description
383004	FortiManager does not fully support management of FAP-C by using the new `fapc-compatibility` command.

Compatibility issues with FortiOS 5.4.2

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS 5.4.2.

Bug ID	Description
396264	Install may fail with `youtube-edu-filter-id` since it has been renamed as `youtube-restrict`.
396270	Install may fail due to default value changes with the following: `rpc-over-http`, `rpc-over-https`, and `mapi-over-https`.

Compatibility issues with FortiOS 5.2.10

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS 5.2.10.

Bug ID	Description
397220	FortiOS 5.2.10 increased the maximum number of the firewall schedule objects for 1U and 2U+ appliances. As a result, a retrieve may fail if more than the maximum objects are configured. **Note**: Compatibility issues with FortiOS 5.2.8/5.2.9 might also apply to FortiOS 5.2.10 devices.

Compatibility issues with FortiOS 5.2.8/5.2.9

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS 5.2.8/5.2.9.

Bug ID	Description
378367	FortiManager may not be able to retrieve all configurations from FortiOS 5.2.8 and subsequent installs may fail.

Compatibility issues with FortiOS 5.2.7

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS 5.2.7.

Bug ID	Description
365757	Retrieve may fail on LDAP User Group if object filter has more than 511 characters.
365766	Retrieve may fail when there are more than 50 portals within a VDOM.
365782	Install may fail on system global optimize or system fips-cc entropy-token.

Compatibility issues with FortiOS 5.2.6

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS 5.2.6.

Bug ID	Description
308294	1) New default wtp-profile settings on FOS 5.2.6 cause verification errors during installation. 2) FortiManager only supports 10,000 firewall addresses while FortiOS 5.2.6 supports 20,000 firewall addresses.

Compatibility issues with FortiOS 5.2.1

The following table lists interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS version 5.2.1.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.

Bug ID	Description
263896	If it contains the certificate: `Fortinet_CA_SSLProxy` or `Fortinet_SSLProxy`, `retrieve` may not work as expected.

Compatibility issues with FortiOS 5.2.0

The following table lists known interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS version 5.2.0.

Bug ID	Description
262584	When creating a VDOM for the first time it fails.
263949	Installing a VIP with port forwarding and ICMP to a 5.2.0 FortiGate fails.

Compatibility issues with FortiOS 5.0.5

The following table lists known interoperability issues that have been identified with FortiManager version 5.2.1 and FortiOS version 5.0.5.

Bug ID	Description
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.5 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Compatibility issues with FortiOS 5.0.4

The following table lists known interoperability issues that have been identified with FortiManager version 5.4.1 and FortiOS version 5.0.4.

Bug ID	Description
226064	Attempting to install time zones 79 and 80 fails. These time zones were added in FortiOS 5.0.5.
226078	When the password length is increased to 128 characters, the installation fails.
226098	When installing a new endpoint-control profile, installation verification fails due to default value changes in FortiOS 5.0.5.
226102	If DHCP server is disabled, installation fails due to syntax changes in FortiOS 5.0.5.

Bug ID	Description
226203	Installation of address groups to some FortiGate models may fail due to table size changes. The address group table size was increased in FortiOS 5.0.5.
226236	The `set dedicated-management-cpu enable` and `set user-anonymize enable` CLI commands fail on device install. These commands were added in FortiOS 5.0.5.
230199	FortiManager allows the creation of a new FAP-320C WTP profile on a FortiOS 5.0.4 device causing the install to fail. FAP-320C is new for FortiOS 5.0.6.

Resolved Issues

The following issues have been fixed in 5.4.1. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
294183	Config Status is not updated following an auto update from FortiGate.
308211	After user imports a policy package, another policy package status changes to “modified”.
355528	When users remove a FortiGate with a FortiExtender attached, the FortiExtender device is not removed.
296595	Editing the HA-mgmt interface under Device Manager triggers Web Server Error 500.
356163	FOS-VM auto-register may not be completely successful.
363354	Policy import may fail due to GTP profile address group.
365156	Interface can be created with a name containing a trailing space.
357457	Users cannot assign multiple AS numbers for set-aspath when configuring a router route-map rule.
364495	FortiManager does not automatically promote an unregistered device with an existing matching Model Device.
306325	FortiManager does not store secondary IP address in FortiGate revisions.
369642	Re-installing policy may not be working on GUI.
364256	When a Wifi SSID interface is edited, the authentication group or server may be removed.
365673	FortiManager may remove the newline characters in `web-proxy explicit pac-file-data`.
372915	Auto update may not work.
305403	The *Create revision* checkbox may not be selected in Install Wizard when `create-revision` is set to `enabled` in CLI.
371136	In the prefix-list, users may not be able to specify *LE* with a blank *GE* value.

Bug ID	Description
306235	FortiManager may not list available interfaces on GUI when users are creating a hardware switch.
374585	FortiManager may not be able to retrieve config from FortiGate.
302373	The icon of log encryption status in Device Manager may be missing.
368324	Users may not be able to enable *Automatic link the real device* with the model device after the model device is created.
371490	Users may not be able to edit an interface when its IP subnet is overlapping with the IP of `ha-mgmt-interface`.
375317	Wrong device may be shown in the popup in *Firmware Upgrade* page after user selects a device from the filtered result.
371296	DHCP Relay Server IPs may not be installed to FortiGate.
356627	Users may not be able to configure advanced settings of aggregate interfaces from GUI.
357546	IPSec Phase 1 config page may refresh unexpectedly.
364121	*Firmware* tab may show all devices while it should only display the devices within the group.
377040	Session-helper table indices may not be maintained correctly on FortiManager.
374318	Default configuration values for Route-map on FortiManager may be different from that on FortiGate.
371680	*Create New* and *Edit* buttons of MAC address Access Control List may not work in Interface Edit page.
370403	Users may not be able to configure concurrent install limit and timeout value for firmware upgrade in firmware manager.

Global ADOM

Bug ID	Description
354336	When rating overrides are created in Global Policy, they are not assigned to local ADOM after the policy is assigned to local ADOM.
369640	FortiManager may install header policies in the wrong order to FortiGate.
377380	Policies in Global ADOM may not be able to be moved by *Cut* and *Paste below* or *Paste above*.

Policy and Objects

Bug ID	Description
309152	When workspace is enabled, FortiManager cannot detect the change of a dynamic address group.
355672	FortiManager should allow overlapping a VIP that has “src-filter” set and with “any” in the same policy.
288655	The "policy interface selection" drop-down list may not show zones or interfaces.
365911	Policy package install may fail due to URL prefixes in `ftgd-local-ratings`.
368788	Local rating category override with a trailing slash cannot be edited or deleted.
364213	The “match-vip” setting in a policy is not installed to FortiGate from FortiManager.
157969	With the command to `unset associated-interface` of a firewall address leads to deletion of firewall policies using this address.
367446	Adding or removing groups in FSSO causes the user group to lose all its members.
356014	Users may be allowed to create Explicit proxy with application control profile with category 6 "Proxy blocked".
368133	LDAPS query may not work under Policy and Objects.
371082	The default mapping configuration of a policy interface may not work.
369599	Following an upgrade from 5.2.2, FortiManager may not be able to install ssl.vdom interface that maps a zone to FortiGate.
363970	Users may not be able to open the result of Policy Consistency Check.
294547	The policy package name-length limit is not consistent for import and policy table.
367451	Changing zone name during import process may cause policy installation to FortiGate to fail later.
367689	Users may not be able to add or delete FortiGate in Installation target list.
299953	Users may not be able to configure *other-application-log* value on an application control profile by using the FortiManager GUI.
369398	The *proxy* option may not be set when web filter profile is selected.
309017	In workflow mode, display option changes may not get saved.

Bug ID	Description
356962	*Device group* may be missing for policy package *Source Device* field in right-hand side object selection pane.
374987	Zone mapping may not support multiple interfaces inside Install Wizard.
357099	Policy for policy-based IPSec VPN may not be installed to FortiGate when zone is used in destination interface.
308892	LDAP user search on FortiManager may be *cn* based only from GUI.
305405	Policy hit count may not display details.
308503	Users may not be able to create dynamic mapping for FSSO.
377560	Adding a UTM profile from right-hand-side object selection list in policy table list may not work.

Script

Bug ID	Description
235769	Script may stop running if it contains `append` command.
364436	Users may be able to add duplicate objects to ADOM database when using a script.
370760	Running a script to a group of devices may hang at 1%.

Services

Bug ID	Description
310097	Users may not be able to access FortiManager when many FortiGate units request updates.
355161	Downstream FortiManager may not be able to get account IDs for licenses.
310069	The random setting of AV/IPS update-schedule time does not work.
364406	FortiGuard Server may run out of memory and crash.
369636	Object 05000000IRDB00101 may not be shown on GUI.

System Settings

Bug ID	Description
369068	Users may see incorrect out-of-sync configuration status reported in Event logs during a Policy Package install.
307237	Admin user cannot log in via JSON API using two-factor authentication.
355150	FortiManager HA gets out-of-sync when user moves a widget on Dashboard page.
365800	FortiManager does not support the time zone GMT +13:00 Samoa with DST.
365953	Hyperlinks in approval emails sent by FortiManager workflow mode may not be redirected to HTTPS.
368149	Admin users may not be able to run diagnose sniffer when they have Read Only permissions to System Settings.
373014	Users may not be able to change settings on Admin Settings page under System Settings.
371995	Users with *Super_user* profile from Radius server may not be able to access any ADOM.
307035	The calendar in system time setting may be difficult to view completely
373004	ADOM config changes may reset *Display Options* for *Device Manager* and *Policy Package & Objects* pages.
364053	Root certificate is required when configuring LDAPS under LDAP server settings on FortiManager.
375948	Restricted admin may be able to view Policy Packages.
274940	Admin users with Read-Write access to Terminal manager and Read-Only access to others for Device manager may not be able to use *Connect to CLI* function in FortiGate Dashboard.
373856	Admin users with Read-Only access may not be able to view policy and policy object details when the ADOM is unlocked under workspace mode.

VPN Console

Bug ID	Description
363281	Users may fail to configure VPN as an IPSec IPv6 interface.

Bug ID	Description
357569	IPSec Phase1 objects may be created without interface.
369531	Disabling Web Mode in FortiManager may result in an error during installation, if default heading value has been changed.
372627	Summary network may be shown on create / edit VPN star spoke page.
373497	For FortiGates upgraded in 5.0 ADOMs, the certificate authentication in VPN settings may be removed and be replaced by `psk=null`.
374453	Encryption and hashing algorithm drop lists may be empty in IPSec phase1 configurations.
372516	Users may not be able to set local id from GUI for VPN members.
373495	Some Diffie-Hellman groups are missing in IPsec Phase2 configuration page.

Others

Bug ID	Description
292570	When there are different certificates, FortiManager may not use the stronger one for FGFM tunnel establishment.
267976	Users cannot copy objects from ADOM database to Device database by JSON API.
368050	The `obj seq` is not returned in JSON API response for policies.
370925	FortiManager HA Slave may be able to run `diag cdb check adom-integrity`.
369939	FortiManager may not be able to upgrade a 5.0 ADOM to 5.2.
286467	Restoring an encrypted revision downloaded from FortiManager into FortiGate may fail.
372455	The "diag dvm proc list" may falsely report "PROCESS IS NOT RESPONDING".

Common Vulnerabilities and Exposures

Bug ID	Description
371045	FortiManager 5.4.1 is no longer vulnerable to the following CVE-References: • 2016-2176 • 2016-2109 • 2016-2108 • 2016-2107 • 2016-2106 • 2016-2105 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in 5.4.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
302345	Users may not be able to add FortiAnalyzer or FortiSandbox from root ADOM.
377929	FortiManager may not be able to provide AV/IPS update for FortiSandbox 2.2.1.
377913	*tertiary-secret* in radius server configuration may not be installed to FortiGate.
377025	Policy package status of a multi-vdom FortiGate AP cluster may show *unknown* after a fail-over.
377259	Adding a FortiGate may fail if the device is also added as an unregistered device during the process. **Workaround**: Please remove the central management configurations on the FortiGate before adding a device.
378564	FortiManager does not fully support FortiGate-500D with FortiOS 5.4.1 installed.

FortiClient ADOM

Bug ID	Description
379088	When creating a new interface, FortiManager should generate the CLI: `set endpoint-compliance enable`. **Workaround**: Please create the new interface on FortiClient and retrieve the new configurations.

Policy and Objects

Bug ID	Description
369851	Deleting a device may not remove its associated mappings.

Bug ID	Description
304932	Column Filter is unavailable for 5.2 or 5.4 ADOM.
379245	Policy cut and paste does not work in section view.
380336	When switching to session view, policy order is based on policy ID instead of sequence number.

System Settings

Bug ID	Description
269571	PKI users may not be able to log into the Restricted Admin Portal.
375204	When an administrator is assigned to a group and it has wildcard enabled, FortiManager may prompt the `Failed to Start` error during login.

Others

Bug ID	Description
298446	FortiManager should synchronize FortiMeter data to all slave units within a HA cluster.
377217	During upgrade, FortiManager may require extra time to upgrade large databases.
375575	FortiManager may lose configuration or VM license after upgrade. **Workaround**: Please see the following special notice: System Configuration or VM License is Lost after Upgrade on page 9.
388071	FortiManager may not be able to render a proper web GUI page when making a change.

FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiClient (Windows)	• 5.0.0 and later • 5.2.0 and later • 5.4.0 and later	✓		✓	
FortiClient (Windows)	• 4.3.0 and later	✓			
FortiClient (Windows)	• 4.2.0 and later	✓	✓		✓
FortiClient (Mac OS X)	• 5.0.1 and later • 5.2.0 and later	✓		✓	
FortiMail	• 4.2.0 and later • 4.3.0 and later • 5.0.0 and later • 5.1.0 and later • 5.2.0 and later	✓	✓		
FortiSandbox	• 1.2.0, 1.2.3 • 1.3.0 • 1.4.0 and later	✓			

Platform	Version	Antivirus	AntiSpam	Vulnerability Scan	Software
FortiWeb	• 5.0.6 • 5.1.4 • 5.2.0 and later • 5.3.0	✓			

To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
   set status enable
end
```

FORTINET®

High Performance Network Security